CYBER THREATS

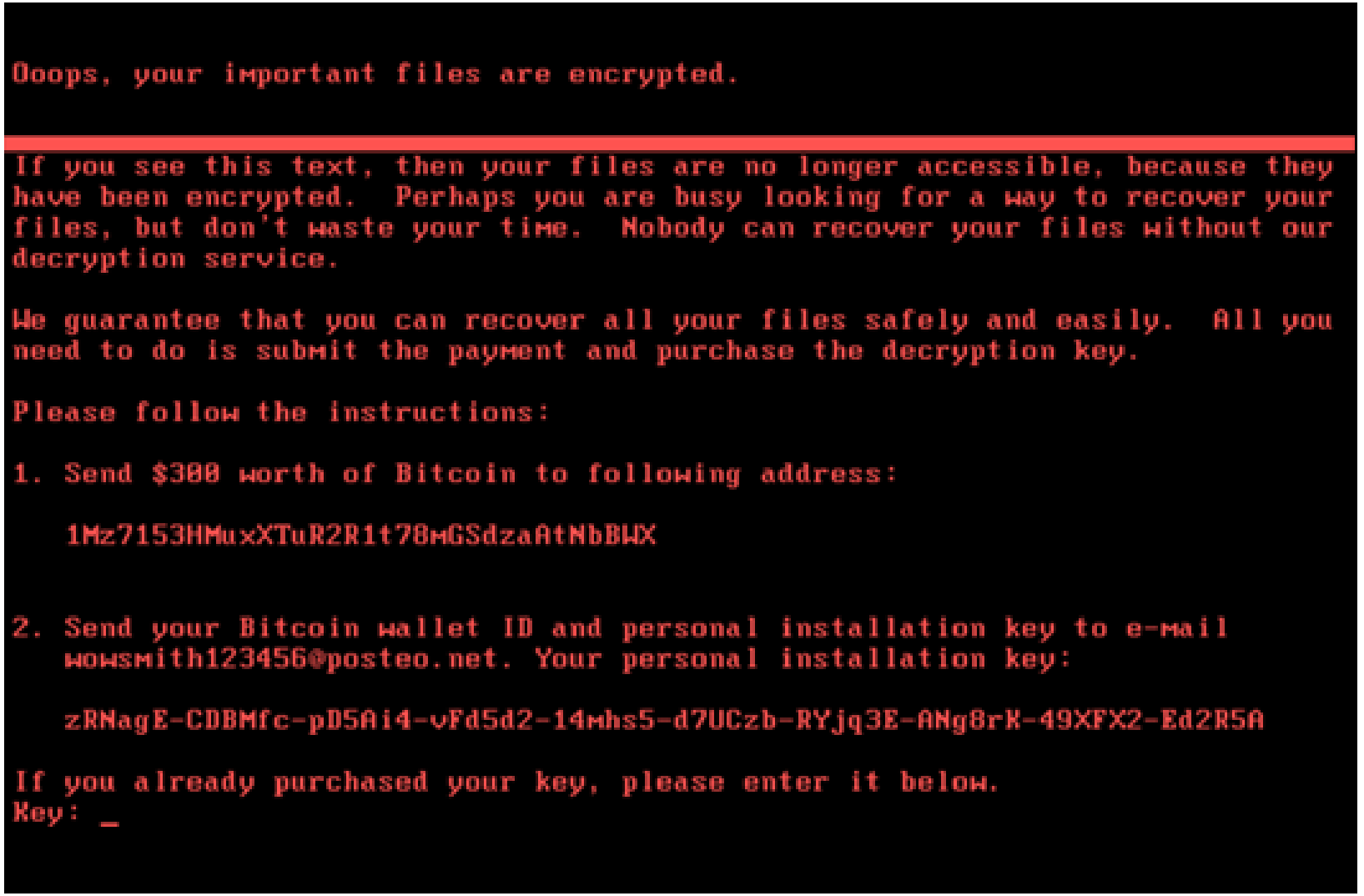
A CLEAR AND PRESENT DANGER

Carl Peers – SVP Human Resources, OneBlood

HAPPY BIRTHDAY!

ITS YOUR BIRTHDAY WEEKEND, YOU NOTICE SEVERAL EMAILS FROM IT ABOUT A SYSTEMS OUTAGE BUT DON’T THINK TOO MUCH OF IT…

RANSOMWARE


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A
If you already purchased your key, please enter it below.
Key: _

TERMINOLOGY

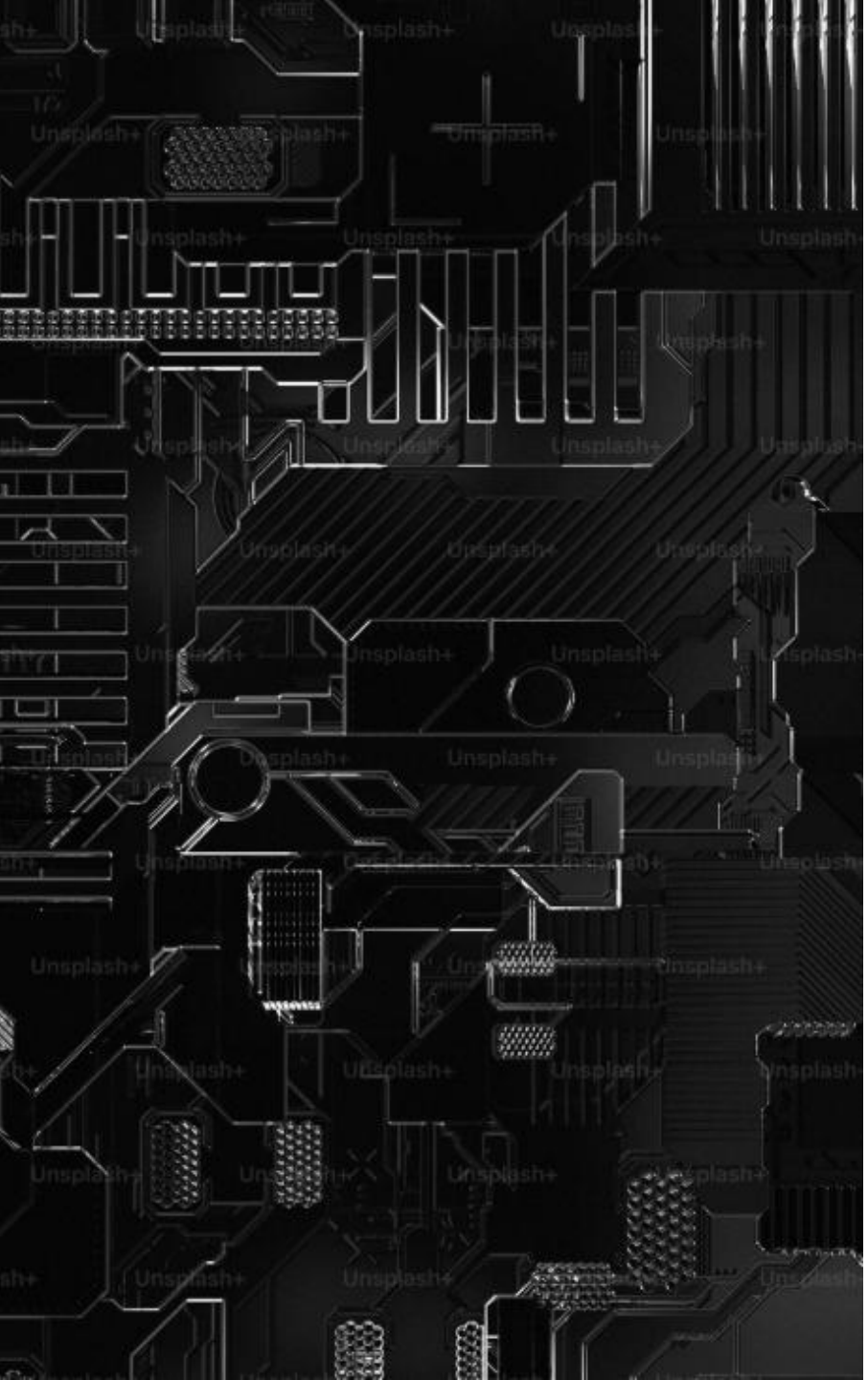
- Ransomware - A form of malware designed to encrypt files on a device, rendering them and the systems that rely on them unusable.

HOW DOES IT WORK

- Break into your system
  - **Social Engineering**
  - **Vulnerabilities**
  - **Employee/Vendor Mistake**
- **Learn your system**
  - **Locate data**
  - **Locate backups**
  - **Stealth Tactics**

HOW DOES IT WORK

- Plan their Exit - Execute
  - **Exfiltrate data**
  - **Create Persistence**
  - **Encrypt Data**
  - **Leave the Note**



IMPACT

- Typically, All or most systems are down
- Must fall back to manual processes
- Theat Actor wants money to give you decryption key
- Sometimes, threat actor wants money again to not leak your data

RANSOMWARE CASES

First Quarter 2025

- 278 disclosed attacks
- 2124 undisclosed attacks
- Healthcare #3 - #1 disclosed
- Non-Profits – 33 incidents vs 16 Q4
- Clop, RansomHub, Akira

Why the Growth?

- $$$
- RAAS – Ransomware as a Service
- Organized Business

RESIST

- Build a Culture of Security
  - Leader Responsible for Security
  - Leadership Buy in
  - Continuous Security Training/Testing
  - Vulnerability Assessments / Audits
- Security Built in from the Beginning
  - Part of new project requests
  - Change Control
- Zero Trust Framework

- Immutable Backups
- Patch Management
- End-Point Protection (EDR), SIEM, Monitoring
- Encryption
- Multi-Factor Authentication (MFA), Strict Access Controls, Least Privilege
- Data Loss Prevention (DLP)
- Incident Response Plan – Complete & Practiced

RECOVER

- Incident Response Plan
  - Contacts
    - Legal
    - Cyber Insurance
    - Recovery/Forensic Consultants
- Immutable Backups
- List of all Digital Assets
  - All Assets prioritized
  - Dependencies Identified

- Communication Plan
- Downtime Policies / Procedures
- Have Extra Storage Available
- Password Resets for everything
- Shift Planning

TRAINING PROGRAMS FOR STAFF

Importance of Training

Regular training empowers employees to identify security threats, enhancing overall organizational safety and awareness.

Recognizing Threats

Training helps staff recognize potential security threats, ensuring timely and appropriate responses to incidents.

Culture of Vigilance

Consistent training fosters a culture of vigilance, where employees actively participate in maintaining a secure environment.

RECOGNIZING PHISHING AND SOCIAL ENGINEERING

Importance of Awareness

Recognizing phishing attempts is crucial for protecting sensitive information and preventing ransomware attacks.

Common Phishing Tactics

Phishing tactics often involve deceptive emails or messages designed to trick individuals into revealing personal information.

Social Engineering Risks

Social engineering exploits human psychology to manipulate individuals into divulging confidential information.

PROMOTING A CULTURE OF SECURITY AWARENESS

Employee Engagement

Engaging employees in security awareness training is essential for fostering a proactive security culture within the organization.

Reporting Suspicious Activities

Encouraging employees to report suspicious activities helps in identifying and mitigating potential security threats early.

Continuous Improvement

Promoting a culture of continuous improvement in security practices ensures the organization stays ahead of emerging threats.

LESSONS FOR HUMAN RESOURCES

Payroll and Expenses

Build a plan for how you will handle with all systems down

Communication

Establish a means of communication to your employees

Downtime Process Data Entry

Consider downtime procedures, resources to enter the data and coordination of those resources

CONCLUSION

Ransomware Threat

Ransomware continues to pose a significant threat to organizations, impacting data security and operations.

Comprehensive Security Measures

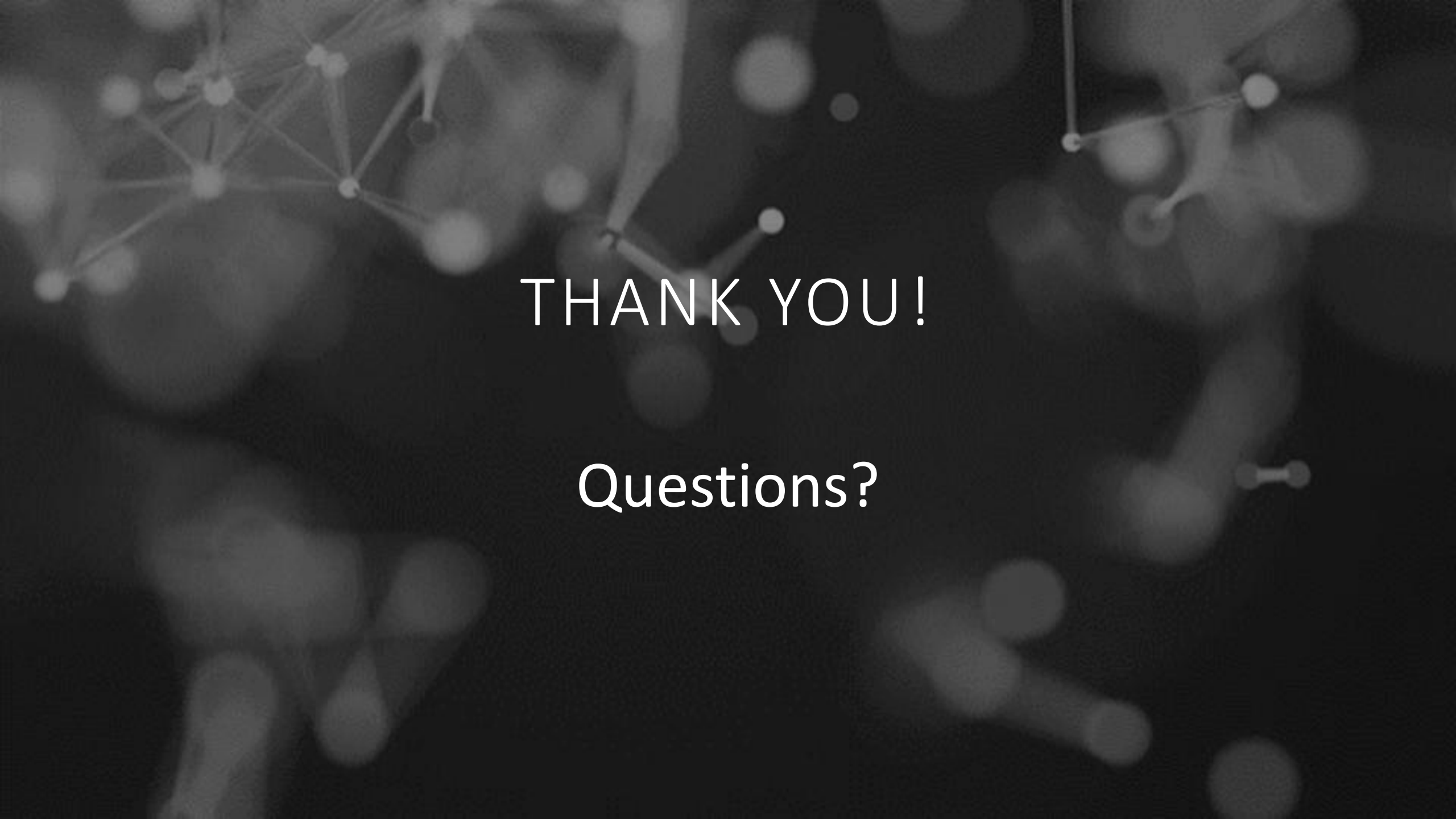
Implementing comprehensive security measures is vital to protect sensitive information from ransomware attacks.

Incident Response Planning

Having a well-defined incident response plan helps organizations effectively respond to ransomware incidents and minimize damage.

Employee Education

Educating employees about security best practices can significantly reduce the risk of ransomware attacks.


THANK YOU!
Questions?